## Appendix E

## Hardware / Network Information

This appendix is comprised of four elements:

- State of NJ Three Tier Network Architecture
- *E*-Business Technical Architecture
- *E*-Government Technical Architecture –
  Portal and Authentication Model
- Division on Civil Rights Current Infrastructure

# Introduction to the State of NJ three-tier network architecture

The State of NJ has implemented a three-tier server side network architecture to provide state-of-the-art security design to the State's core Garden State Network resources.

While the physical implementation is actually much more complex than the attached diagram, conceptually you can view the architecture as three firewalls protecting our core network from the Internet world.

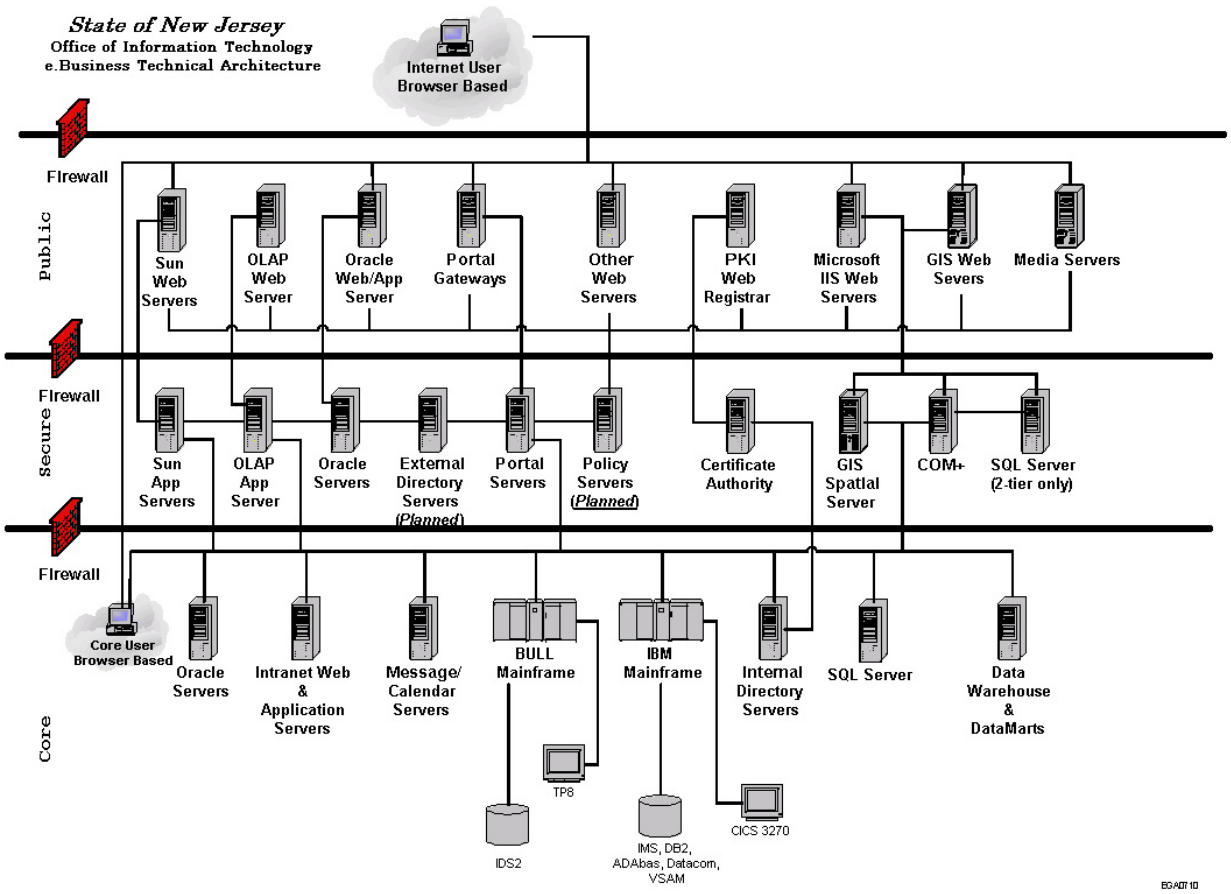
Coordination and integration with the myNJ Portal as the 'one face of government' and leveraging its ability to authenticate and authorize targeted user communities users across many diverse applications is encouraged.

According to our security policy, an Internet user can only communicate with servers on the Public tier, and typically only via HTTP or HTTPS. A Public tier server can only communicate with a Secure tier server, and only a Secure tier server can communicate with core network. A server or workstation can communicate with any device on a higher layer, and the response can come back to only that originating device.

Therefore, in communicating downward in the model from the Internet, at each tier there must be a process, which takes a request and hands it down to the next layer. Typically, this model fits well with distributed application design, where tier 1 handles presentation, tier 2 handles business logic, and tier 3 houses the data. (Web servers, Application servers, Data servers.)

Two tier applications are accommodated in this model by placing the data on the second tier, as was the universal practice up until a few years ago. One tier applications (highly discouraged) are accommodated by placing all components on the first tier.

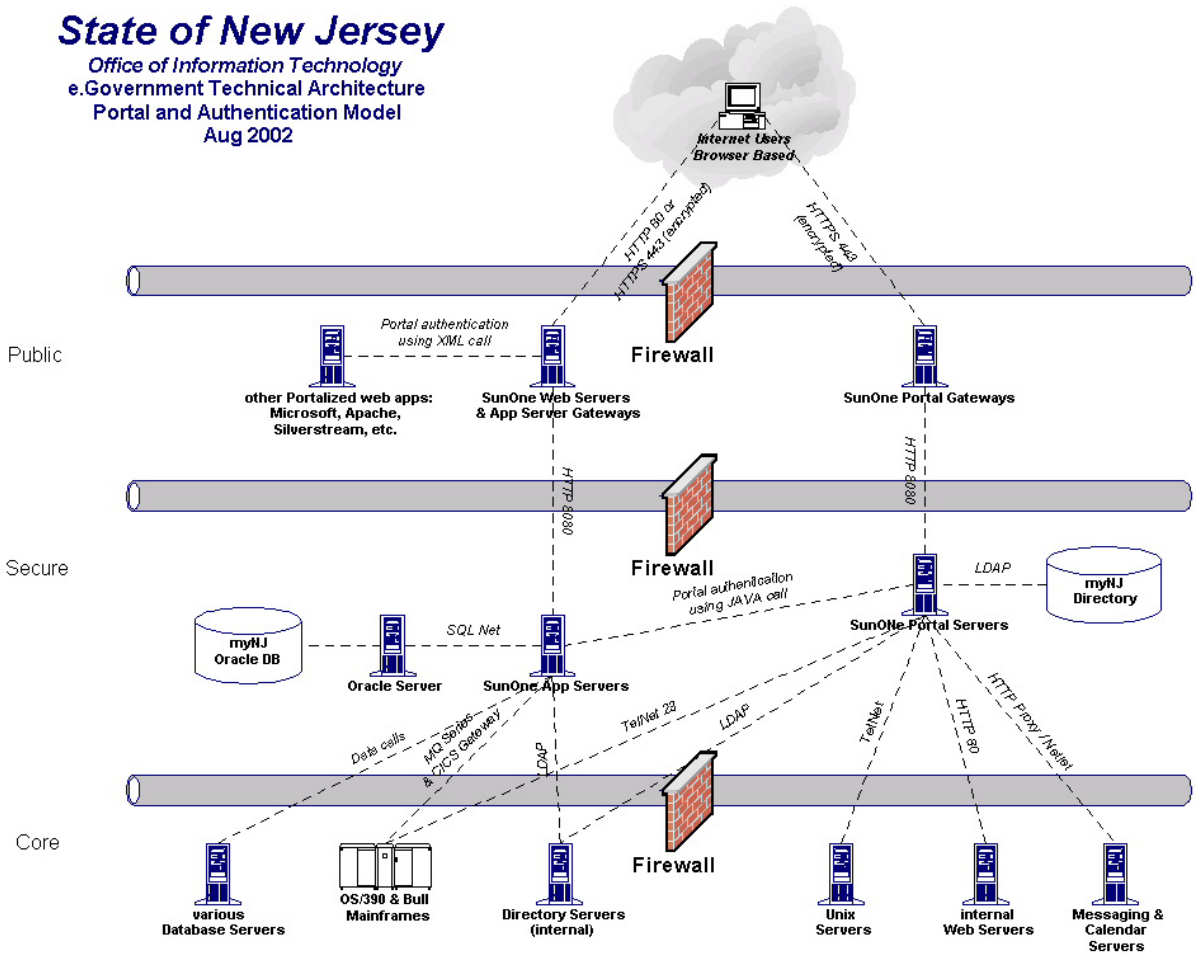
Tunneling, simple pass-through proxy, 'double tier hops', and other techniques that do not apply policy or process to an inward bound communication at each tier, are not allowed. To do so would compromise the integrity of all remaining applications that do follow the security policy.

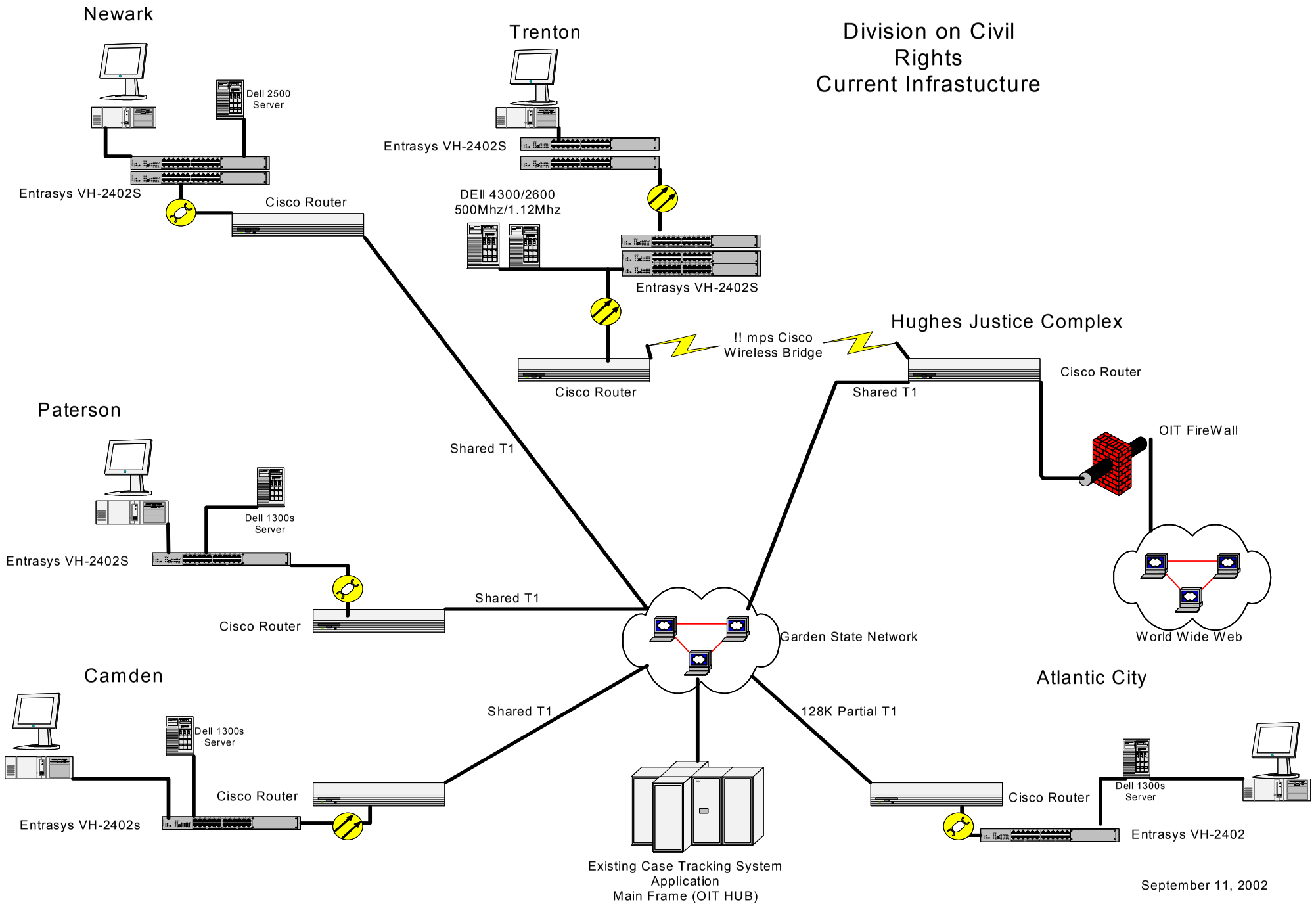

State of New Jersey
Office of Information Technology
e.Business Technical Architecture
Internet User Browser Based
Firewall
Public
Sun Web Servers
OLAP Web Server
Oracle Web/App Server
Portal Gateways
Other Web Servers
PKI Web Registrar
Microsoft IIS Web Servers
GIS Web Severs
Media Servers
Firewall
Secure
Sun App Servers
OLAP App Server
Oracle Servers
External Directory Servers (Planned)
Portal Servers
Policy Servers (Planned)
Certificate Authority
GIS Spatial Server
COM+
SQL Server (2-tier only)
Firewall
Core User Browser Based
Oracle Servers
Intranet Web & Application Servers
Message/ Calendar Servers
BULL Mainframe
IBM Mainframe
Internal Directory Servers
SQL Server
Data Warehouse & DataMarts
Core
TP8
IDS2
IMS, DB2, ADAbas, Datacom, VSAM
CICS 3270
EGA07110

# State of New Jersey

*Office of Information Technology*

e.Government Technical Architecture
Portal and Authentication Model
Aug 2002




Division on Civil Rights
Current Infrastucture
Newark
Dell 2500 Server
Entrasys VH-2402S
Cisco Router
Trenton
Entrasys VH-2402S
DEll 4300/2600
500Mhz/1.12Mhz
Entrasys VH-2402S
!! mps Cisco Wireless Bridge
Cisco Router
Hughes Justice Complex
Cisco Router
Shared T1
OIT FireWall
World Wide Web
Paterson
Dell 1300s Server
Entrasys VH-2402S
Cisco Router
Shared T1
Shared T1
Garden State Network
Camden
Dell 1300s Server
Entrasys VH-2402s
Cisco Router
Shared T1
128K Partial T1
Existing Case Tracking System
Application
Main Frame (OIT HUB)
Atlantic City
Dell 1300s Server
Cisco Router
Entrasys VH-2402
September 11, 2002